PRIME LEHMER AND LUCAS NUMBERS WITH COMPOSITE INDICES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. Let $R(L,M)$ and $U(P,Q)$ denote the Lehmer and Lucas sequences, respectively. It is shown that if $R(L,M)$ and $U(P,Q)$ are nondegenerate, then $R_n(L,M)$ and $U_n(P,Q)$ can be prime for composite n only if $n \in \{4,6,8,9,10,14,15,21,25,26,49,65\}$. Moreover, all instances in which $R_n(L,M)$ or $U_m(P,Q)$ are prime are explicitly given when $n \in \{14,15,21,26,49,65\}$ and $m \in \{6,8,10,15,25,26,65\}$.

1. Introduction

Consider the prime values of the Fibonacci sequence $\{F_n\}$, which is both a Lehmer and a Lucas sequence. We observe that F_n is known to be prime for 32 prime indices, the largest of which is $n = 81839$, but is prime for only one composite index, namely $n = 4$ (see [12]). It is conjectured that F_n is prime for infinitely many prime indices n (see [8], pp. 362–364). We will prove that apart from the exceptional cases in which the sequences are degenerate, there are only 12 composite indices n for which there exists a Lehmer or Lucas number with that index for which its value is prime, namely the indices $n \in \{4,6,8,9,10,14,15,21,25,26,49,65\}$. We will explicitly exhibit all the finitely many instances in which this happens when $n \in \{14,15,21,26,49,65\}$ in the case of the Lehmer sequences and $n \in \{6,8,10,15,25,26,65\}$ in the case of the Lucas sequences.

Throughout this paper, p will denote a prime and ε will be assumed to be a member of the set $\{-1,1\}$. To proceed, we will need to define the Lehmer and Lucas sequences and present some of their properties.

Let $R(L,M) = \{R_n(L,M)\}$ and $S(L,M) = \{S_n(L,M)\}$ denote the Lehmer and the companion Lehmer sequence, respectively, defined by

$$R_n = \begin{cases} \frac{\gamma^n-\delta^n}{\gamma-\delta}, & n \text{ odd}, \\ \frac{\gamma^n-\delta^n}{\gamma^2-\delta^2}, & n \text{ even}, \end{cases} \qquad S_n = \begin{cases} \frac{\gamma^n+\delta^n}{\gamma+\delta}, & n \text{ odd}, \\ \gamma^n+\delta^n, & n \text{ even}, \end{cases} \tag{1.1}$$

where $n \ge 0$, L and M are rational integers, and γ and δ are the roots of the equation

$$x^2 - \sqrt{L}x + M = 0. \tag{1.2}$$

The discriminant $K = K(L,M)$ of both $R(L,M)$ and $S(L,M)$ is given by $K(L,M) = L - 4M$. In the formulas (1.1), we assume that both $K = (\gamma-\delta)^2$ and $L = (\gamma+\delta)^2$ are nonzero. It is easily seen that $R(L,M)$ and $S(L,M)$ satisfy the recursion relations

$$R_{n+2} = \begin{cases} LR_{n+1} - MR_n & \text{for } n \text{ odd}, \\ R_{n+1} - MR_n & \text{for } n \text{ even} \end{cases} \tag{1.3}$$

This paper was supported by the Project RVO 67985840.

with initial terms $R_0 = 0$, $R_1 = 1$, and

$$S_{n+2} = \begin{cases} S_{n+1} - MS_n & \text{for } n \text{ odd,} \\ LS_{n+1} - MS_n & \text{for } n \text{ even} \end{cases} \tag{1.4}$$

with initial terms $S_0 = 2$, $S_1 = 1$. If $K(L, M) = 0$ or $L = 0$, we use equations (1.3) and (1.4) to define $R(L, M)$ and $S(L, M)$ rather than the equations in (1.1). Unless stated otherwise, we assume that $R(L, M)$ and $S(L, M)$ are nondegenerate, that is, $M = \gamma\delta \neq 0$ and γ/δ is not a root of unity. Note that $R_n(L, M) = 0$ for some $n > 0$ only if $R(L, M)$ is degenerate.

D. H. Lehmer in 1930 (see [5]), defined the Lehmer sequences $R(L, M)$ and $S(L, M)$ as generalizations of the Lucas sequence $U(P, Q)$ and companion Lucas sequence $V(P, Q)$, defined by

$$U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n(P, Q) = \alpha^n + \beta^n, \tag{1.5}$$

where $n \geq 0$, P and Q are rational integers, and α and β are the roots of

$$x^2 - Px + Q = 0. \tag{1.6}$$

The discriminant $D = D(P, Q)$ of both $U(P, Q)$ and $V(P, Q)$ is given by $D = P^2 - 4Q = (\alpha - \beta)^2$. Similarly to the case of the Lehmer sequence, we assume unless stated otherwise that $U(P, Q)$ and $V(P, Q)$ are nondegenerate, i.e., $Q = \alpha\beta \neq 0$ and α/β is not a root of unity. The sequences $U(P, Q)$ and $V(P, Q)$ both satisfy the recursion relation

$$W_{n+2} = PW_{n+1} - QW_n \tag{1.7}$$

with initial terms $U_0 = 0$, $U_1 = 1$ and $V_0 = 2$, $V_1 = P$.

The Lucas numbers are related to the Lehmer numbers by means of the following formulas (see [7], p. 436):

$$U_n(P, Q) = \begin{cases} R_n(P^2, Q) & \text{for } n \text{ odd,} \\ PR_n(P^2, Q) & \text{for } n \text{ even} \end{cases} \tag{1.8}$$

and

$$V_n(P, Q) = \begin{cases} PS_n(P^2, Q) & \text{for } n \text{ odd,} \\ S_n(P^2, Q) & \text{for } n \text{ even.} \end{cases} \tag{1.9}$$

Note that $R_n(1, M) = U_n(1, M)$ and $S_n(1, M) = V_n(1, M)$ for all n.

Example 1.1. For later reference, we make use of the recursion relations given in (1.3) and (1.4) to derive the first seven terms of both $R(L, M)$ and $S(L, M)$ in terms of L and M:

$$\begin{aligned} &R_0 = 0,\ R_1 = R_2 = 1,\ R_3 = L - M,\ R_4 = L - 2M, \\ &R_5 = L^2 - 3LM + M^2,\ R_6 = L^2 - 4LM + 3M^2, \end{aligned} \tag{1.10}$$

$$\begin{aligned} &S_0 = 2,\ S_1 = 1,\ S_2 = L - 2M,\ S_3 = L - 3M,\ S_4 = L^2 - 4LM + 2M^2, \\ &S_5 = L^2 - 5LM + 5M^2,\ S_6 = L^3 - 6L^2M + 9LM^2 - 2M^3. \end{aligned} \tag{1.11}$$

The proposition below is well-known and follows from (1.1) and (1.5) (see [5], pp. 420–421).

Proposition 1.2.

(i) *If* $m \mid n$ *then* $R_m(L, M) \mid R_n(L, M)$ *and* $U_m(P, Q) \mid U_n(P, Q)$.
(ii) *If* $m \mid n$ *and* n/m *is odd, then* $S_m(L, M) \mid S_n(L, M)$ *and* $V_m(P, Q) \mid V_n(P, Q)$.
(iii) $R_n(-L, -M) = (-1)^{\lfloor (n-1)/2 \rfloor} R_n(L, M)$.
(iv) $U_n(-P, Q) = (-1)^{n-1} U_n(P, Q)$.
(v) $R_{2n}(L, M) = R_n(L, M) S_n(L, M)$.

(vi) $U_{2n}(P,Q) = U_n(P,Q)V_n(P,Q)$.
(vii) $V_{2n}(P,Q) = V_n^2(P,Q) - 2Q^n$.

Since $R_1(L,M) = U_1(P,Q) = 1$, it is clear from Proposition 1.2 (i) that $|R_n(L,M)|$ or $|U_n(P,Q)|$ can be prime if n is prime. However, in rare instances $|R_n(L,M)|$ or $|U_n(P,Q)|$ can be prime if n is a composite number. Since we are interested in when $|R_n(L,M)|$ and $|U_n(P,Q)|$ are prime, we will assume throughout this paper $L \geq 0$ and $P \geq 0$ by virtue of Proposition 1.2 (iii) and (iv).

In the next section, along with other results, we will determine all instances in which $R(L,M)$ or $U(P,Q)$ is degenerate and $|R_n(L,M)|$ or $|U_n(P,Q)|$ is prime for composite n. For reference, the following proposition lists all cases in which $R(L,M)$ or $U(P,Q)$ are degenerate.

Proposition 1.3. *Consider the Lehmer sequence $R(L,M)$ and the Lucas sequence $U(P,Q)$. Let N be a positive integer. Then*

(i) *$R(L,M)$ is degenerate if and only if $LM = 0$ or (L,M) is of the form (N,N), $(2N,N)$, $(3N,N)$, or $(4N,N)$,*
(ii) *$U(P,Q)$ is degenerate if and only if $PQ = 0$ or (P,Q) is of the form (N,N^2), $(2N,2N^2)$, $(3N,3N^2)$ or $(2N,N^2)$.*

Proof. Part (i) is proved in [5], pp. 425–426, for the case in which $\gcd(L,M) = 1$. The result in which $\gcd(L,M) > 1$ follows immediately. Part (ii) is proved in [11], p. 613. □

Lemma 1.4. *Let $R(L,M)$ be a degenerate Lehmer sequence for which* $\gcd(L,M) = 1$. *Let $n \geq 0$ and $k \geq 0$. Then*

(i) *$(L,M) = (0,\varepsilon)$, $(1,0)$, $(1,1)$, $(2,1)$, $(3,1)$, or $(4,1)$.*
(ii) *If $(L,M) = (0,\varepsilon)$, then $R_{2n} = n(-\varepsilon)^{n-1}$ and $R_{2n+1} = (-\varepsilon)^n$.*
(iii) *If $(L,M) = (1,0)$, then $R_0 = 0$ and $R_n = 1$ for $n \geq 1$.*
(iv) *If $(L,M) = (1,1)$, then $R_n = 0$ for $n = 3k$ and $R_n = (-1)^k$ for $n = 3k + r$, where $r \in \{1,2\}$.*
(v) *If $(L,M) = (2,1)$, then $R_n = 0$ for $n = 4k$ and $R_n = (-1)^k$ for $n = 4k + r$, where $r \in \{1,2,3\}$.*
(vi) *If $(L,M) = (3,1)$, then $R_n = 0$ for $n = 6k$, $R_n = 2(-1)^k$ for $n = 6k + 3$, and $R_n = (-1)^k$ for $n = 6k + r$, where $r \in \{1,2,4,5\}$.*
(vii) *If $(L,M) = (4,1)$, then $R_{2n} = n$ and $R_{2n+1} = 2n + 1$.*

Proof. Part (i) follows from Proposition 1.3 (i). Parts (ii)–(vii) can be established through induction. □

Lemma 1.5. *Let $U(P,Q)$ be a degenerate Lucas sequence for which* $\gcd(P,Q) = 1$. *Let $n \geq 0$ and $k \geq 0$. Then*

(i) *$(P,Q) = (0,\varepsilon)$, $(1,0)$, $(1,1)$, or $(2,1)$.*
(ii) *If $(P,Q) = (0,\varepsilon)$, then $U_{2n} = 0$ and $U_{2n+1} = (-\varepsilon)^n$.*
(iii) *If $(P,Q) = (1,0)$, then $U_0 = 0$ and $U_n = 1$ for $n \geq 1$.*
(iv) *If $(P,Q) = (1,1)$, then $U_n = 0$ for $n = 3k$ and $U_n = (-1)^k$ for $n = 3k + r$, where $r \in \{1,2\}$.*
(v) *If $(P,Q) = (2,1)$, then $U_n = n$ for $n \geq 0$.*

Proof. Part (i) follows from Proposition 1.3 (ii). Parts (ii)–(v) follow by induction. □

2. Main Results

Theorem 2.1. *Consider the Lehmer sequence $R(L, M)$ and the Lucas sequence $U(P, Q)$. Suppose that $\gcd(L, M) = d_1 > 1$ and $\gcd(P, Q) = d_2 > 1$. Then*

(i) $|R_n(L, M)| = p$ *for n composite only if $n = 4$ and $|U_n(P, Q)|$ is never prime for n composite.*

(ii) *If p is any prime, then $|R_4(L, M)| = p$ if and only if $p \mid M$, $M \geq 0$, $L = 2M + \varepsilon p$, and $(M, \varepsilon p) \neq (0, -p)$.*

Proof.

(i) It follows by induction using the recursion relations defining $R(L, M)$ and $U(P, Q)$ that $d_1^k \mid R_n(L, M)$ for $n \geq 2k + 1$ and $d_2^k \mid U_n(P, Q)$ for $n \geq 2k$, where $k \geq 1$. Thus, $d_1^2 \mid R_n(L, M)$ for $n \geq 5$ and $d_2^2 \mid U_n(P, Q)$ for $n \geq 4$. Assertion (i) now follows.

(ii) This follows upon noting that $R_4(L, M) = L - 2M$, $L \geq 0$, and $\gcd(L, M) > 1$ if and only if $p \mid M$.

□

In light of Theorem 2.1, we will assume from here on that $\gcd(L, M) = \gcd(P, Q) = 1$. The remaining results not proved in this section will be proved in Section 4.

Remark 2.2. We note that by Theorem 2.1 (ii), for each prime p there are infinitely many ordered pairs (L, M) such that $L \geq 0$, $\gcd(L, M) > 1$, and $|R_4(L, M)| = p$.

Theorem 2.3. *Let $R(L, M)$ and $U(P, Q)$ be degenerate sequences for which $\gcd(L, M) = \gcd(P, Q) = 1$. Let p be a prime and let $k \geq 1$.*

(i) *If $p = 2$, then $|R_n(L, M)| = 2$ for n composite if and only if $(n, L, M) = (6k + 3, 3, 1)$, $(4, 0, 1)$, $(4, 0, -1)$, or $(4, 4, 1)$.*

(ii) *If p is an odd prime, then $|R_n(L, M)| = p$ for n composite if and only if $(n, L, M) = (2p, 0, 1)$, $(2p, 0, -1)$, or $(2p, 4, 1)$.*

(iii) *$U_n(P, Q)$ is never prime for composite n.*

The proof follows from Lemmas 1.4 and 1.5. By virtue of Theorem 2.3, we will assume from now on that $R(L, M)$ and $U(P, Q)$ are nondegenerate.

Theorem 2.4. *Consider the nondegenerate sequences $R(L, M)$ and $U(P, Q)$. Suppose that $\gcd(L, M) = \gcd(P, Q) = 1$, $K(L, M) = L - 4M > 0$, and $D(P, Q) = P^2 - 4Q > 0$. Then*

(i) *$|R_n(L, M)|$ or $|U_n(P, Q)|$ can be prime for composite n if and only if $n = 4$,*

(ii) *$|R_4(L, M)| = p$ if and only if p is odd, $L = 2M + p$, $-(p - 1)/2 \leq M \leq (p - 1)/2$, and $M \neq 0$,*

(iii) *$|U_4(P, Q)| = p$ if and only if p is odd, $P = 1$, and $Q = (1 - p)/2$.*

Theorem 2.5. *Consider the nondegenerate sequences $R(L, M)$, where $\gcd(L, M) = 1$. Then $|R_n(L, M)|$ can be prime for n composite only if $n \in \{4, 6, 8, 9, 10, 14, 15, 21, 25, 26, 49, 65\}$. Moreover, when $n \in \{14, 15, 21, 26, 49, 65\}$, there are only finitely many ordered pairs (L, M) such that $|R_n(L, M)|$ is prime. All such instances are given as follows:*

(i) *$R_{14}(3, 2) = R_{14}(5, 2) = 13$,*

(ii) *$R_{14}(3, 4) = R_{14}(13, 4) = -71$,*

(iii) *$R_{15}(1, 2) = -89$,*

(iv) *$R_{21}(3, 2) = 379$,*

(v) *$R_{26}(1, 2) = R_{26}(7, 2) = 181$,*

(vi) $R_{49}(13,4) = 30775052320741$,
(vii) $R_{65}(1,2) = -335257649$.

Example 2.6. It is interesting that $|R_n(1,2)|$ is prime for 9 out of the 12 composite indices for which $R_n(L,M)$ can be prime when $R(L,M)$ is nondegenerate and $\gcd(L,M) = 1$. In particular, $R_4(1,2) = -3, R_6(1,2) = 5, R_8(1,2) = -3, R_9(1,2) = -17, R_{10}(1,2) = -11$, $R_{15}(1,2) = -89$, $R_{25}(1,2) = -4049$, $R_{26}(1,2) = 181$, and $R_{65}(1,2) = -335257649$. Moreover, $|R_n(7,2)|$ and $|R_n(3,2)|$ are each prime for 6 composite indices, and $|R_n(5,2)|$ is prime for 5 composite indices. No other nondegenerate Lehmer sequences are prime for as many composite indices. Specifically, $|R_n(7,2)| = |R_n(1,2)|$ for $n \in \{4,6,8,10,26\}$, $R_6(3,2) = -3$, $R_8(3,2) = 7$, $R_9(3,2) = 19$, $R_9(7,2) = -5$, $R_{10}(3,2) = 5$, $R_{14}(3,2) = 13$, $R_{21}(3,2) = 379$, and $|R_n(5,2)| = |R_n(3,2)|$ for $n \in \{6,8,10,14\}$, $|R_{25}(5,2)| = -4649$.

Theorem 2.7. *Consider the nondegenerate Lucas sequence $U(P,Q)$, where $\gcd(P,Q) = 1$. Then $|U_n(P,Q)|$ can be prime for n composite only if $n \in \{4,6,8,9,10,15,25,26,65\}$. Furthermore, when $n \in \{6,8,10,15,25,26,65\}$, there are only finitely many ordered pairs (P,Q) such that $|U_n(P,Q)|$ is equal to a prime. All such cases are given as follows:*

(i) $U_6(1,2) = 5$,
(ii) $U_8(1,2) = -3$,
(iii) $U_{10}(1,2) = -11$,
(iv) $U_{10}(1,3) = 31$,
(v) $U_{15}(1,2) = -89$,
(vi) $U_{25}(1,2) = -4049$,
(vii) $U_{25}(1,3) = 282001$,
(viii) $U_{26}(1,2) = 181$,
(ix) $U_{65}(1,2) = -335257649$.

This is proved in the proof of Theorem 3.1 on pages 254–256 of [6].

Remark 2.8. From the observations made in Example 2.6, we see that $|U_n(1,2)| = |R_n(1,2)|$ is prime for all 9 possible composite indices.

Theorem 2.9. *Let p be an arbitrary prime. Consider the nondegenerate Lehmer sequence $R(L,M)$ for which $\gcd(L,M) = 1$. Then $|R_4(L,M)| = p$ if and only if $L = 2M + \varepsilon p$, where $p \nmid M$, $M \geq (1-\varepsilon p)/2$, and $(L,M) \neq (0,1)$, $(0,-1)$, or $(4,1)$.*

Proof. Noting that $R_4(L,M) = L - 2M$, we find that $|R_4(L,M)| = p$ if and only if

$$L = 2M + \varepsilon p. \tag{2.1}$$

Clearly, if (2.1) holds, then $\gcd(L,M) = 1$ and $L > 0$ if and only if $p \nmid M$ and $M \geq (1-\varepsilon p)/2$. By use of Theorem 2.3, we see that $|R_4(L,M)| = p$ for a degenerate Lehmer sequence $R(L,M)$ if and only if $p = 2$ and $(L,M) = (0,1)$, $(0,-1)$, or $(4,1)$. □

Theorem 2.10. *Consider the nondegenerate Lucas sequence $U(P,Q)$ for which $\gcd(P,Q) = 1$. Then $|U_4(P,Q)| = p$ if and only if p is odd and one of the following conditions occurs:*

(i) $P = 1$ *and* $Q = (1 \pm p)/2$,
(ii) $P = p$ *and* $Q = (p^2 \pm 1)/2$.

Proof. We observe that

$$U_4(P,Q) = U_2(P,Q)V_2(P,Q) = P(P^2 - 2Q). \tag{2.2}$$

Thus, $|U_4(P,Q)| = p$ if and only if $P = 1$ or $P = p$. If $P = 1$ then $P^2 - 2Q = \pm p$, which implies that $Q = (1 \pm p)/2$. If $P = p$ then $P^2 - 2Q = \pm 1$, yielding that $Q = (p^2 \pm 1)/2$. It is clear that p must be an odd prime and that $\gcd(P,Q) = 1$. It follows from Theorem 2.3 (iii) and (2.2) that $U(P,Q)$ is nondegenerate if $|U_4(P,Q)| = p$. □

Theorem 2.11. *Consider the nondegenerate Lehmer sequence $R(L,M)$. Then $|R_6(L,M)| = p$ if and only if p is odd, $M = (p+\varepsilon)/2$, $(p,\varepsilon) \neq (3,-1)$ and one of the following conditions is satisfied:*

(i) $L = (p + 3\varepsilon)/2$,
(ii) $L = (3p + \varepsilon)/2$.

Proof. We note that

$$R_6(L,M) = R_3(L,M)S_3(L,M) = (L-M)(L-3M).$$

Thus, we have either that

$$L - M = \varepsilon, \quad L - 3M = \pm p \tag{2.3}$$

or

$$L - M = \pm p, \quad L - 3M = \varepsilon. \tag{2.4}$$

Clearly, neither of these simultaneous equations can be solved if $p = 2$. Noting that $L > 0$ and $M \neq 0$, we find that if $L - M = \varepsilon$, then $M > 0$ and $L - 3M < 0$, whereas if $L - 3M = \varepsilon$, then $L - M > 0$. We are now able to determine L and M uniquely for given values of p and ε, obtaining the values for L and M given in parts (i) and (ii). It is easily seen from Theorem 2.3 (ii) that the simultaneous equations (2.3) and (2.4) lead to a case in which $|R_6(L,M)| = p$ for a degenerate Lehmer sequence $R(L,M)$ if and only if $(p,\varepsilon) = (3,-1)$. □

Remark 2.12. We say that the ordered pairs of integers (L,M) and (P,Q) are *standard* if $L > 0$, $P > 0$, $\gcd(L,M) = \gcd(P,Q) = 1$, and both $R(L,M)$ and $U(P,Q)$ are nondegenerate. Theorem 2.9 shows that for any prime p, there exist infinitely many standard ordered pairs (L,M) for which $|R_4(L,M)| = p$. Theorem 2.10 demonstrates that for any odd prime p, there exist exactly four standard ordered pairs (P,Q) for which $|U_4(P,Q)| = p$. Theorem 2.11 shows that if $p = 3$, there exist exactly two standard ordered pairs (L,M) such that $R_6(L,M) = p$, whereas if $p \geq 5$, there exist exactly four standard ordered pairs (L,M) such that $|R_6(L,M)| = p$.

We conjecture that for $k = 8, 9, 10$, or 25, there exist infinitely many standard ordered pairs (L,M) for which $|R_k(L,M)|$ is prime. We similarly conjecture that there exist infinitely many standard ordered pairs (P,Q) such that $|U_9(P,Q)|$ is prime. In Section 5, we provide support for these conjectures by means of Schinzel's Hypothesis H and extensive computer calculations.

Theorem 2.13. *Let us consider the nondegenerate Lehmer sequence $R(L,M)$ such that* $\gcd(L,M) = 1$. *Denote by $P_n = U_n(2,-1)$ the nth Pell number and let $Q_n = \frac{1}{2}V_n(2,-1)$. Then $R_8(L,M)| = p$ if and only if at least one of the following two conditions is satisfied:*

(i) $M \geq 2$, $2M^2 - 1 = p$, *and* $L = 2M + \varepsilon$,
(ii) $k \geq 2$, $Q_k = p$, *and* $(L,M) = (Q_{k-\varepsilon}, P_k)$.

Moreover, the set of primes p for which $|R_8(L,M)| = p$ for some standard ordered pair (L,M) has natural density 0 *in the set of primes.*

Theorem 2.14. *Consider the nondegenerate Lehmer sequence $R(L,M)$ and Lucas sequence $U(P,Q)$ for which $\gcd(L,M) = \gcd(P,Q) = 1$. Then $|R_9(L,M)| = p$ for some ordered pair (L,M) if and only if one of conditions (i), (ii), or (iii) holds:*

(i) $(L,M) = (7,2)$, $p = 5$,
(ii) $M \geq 2$, $3M(M^2-1) - 1 = p$, *and* $L = M - 1$,
(iii) $M \geq 2$, $3M(M^2-1) + 1 = p$, *and* $L = M + 1$.

In particular, $|R_9(M-1,M)|$ *and* $|R_9(M+1,M)|$ *are twin primes when both* $3M(M^2-1)-1$ *and* $3M(M^2-1)+1$ *are primes.*

Furthermore, $|U_9(P,Q)| = p$ *if and only if* $(P,Q) = (M, M^2+\varepsilon)$ *for some* M *such that* $(P,Q) \neq (1,0)$ *and*

$$|R_9(M^2, M^2+\varepsilon)| = 3(M^2+\varepsilon)((M^2+\varepsilon)^2-1) - \varepsilon = p. \tag{2.5}$$

Moreover, the set of primes p *for which* $|R_9(L,M)|$ *or* $|U_9(P,Q)| = p$ *for some standard ordered pair* (L,M) *or* (P,Q) *has natural density* 0 *in the set of primes.*

Theorem 2.15. *Let us consider the nondegenerate Lehmer sequence* $R(L,M)$ *such that* $\gcd(L,M) = 1$. *As usual, let* $F_n = U_n(1,-1)$ *and* $L_n = V_n(1,-1)$ *denote the nth Fibonacci number and nth Lucas number, respectively. Then* $R_{10}(L,M)| = p$ *for some ordered pair* (L,M) *if and only if there exists* $k \geq 3$ *and* ε *such that*

$$|S_5(F_{k-2\varepsilon}, F_k)| = |F_{k-2\varepsilon}^2 - 5F_{k-2\varepsilon}F_k + 5F_k^2| = p. \tag{2.6}$$

Moreover, if (2.6) holds, then

$$|R_{10}(F_{k-2\varepsilon}, F_k)| = |R_{10}(L_{k+\varepsilon}, F_k)| = |R_{10}(F_{k+3\varepsilon}, F_{k+\varepsilon})| = |R_{10}(L_k, F_{k+\varepsilon})| = p. \tag{2.7}$$

Corollary 2.16. *Let* $R(L,M)$ *be a nondegenerate Lehmer sequence for which* $\gcd(L,M) = 1$. *Then* $|R_{10}(L,M)| = p$ *for some ordered pair* (L,M) *if and only if there exists* $k \geq 2$ *such that*

$$S_5(F_{k-2}, F_k) = F_{k-2}^2 - 5F_{k-2}F_k + 5F_k^2 = p. \tag{2.8}$$

Furthermore, the set of primes p *for which* $|R_{10}(L,M)| = p$ *for some standard ordered pair* (L,M) *has natural density* 0 *in the set of primes.*

Theorem 2.17. *Let us consider the nondegenerate Lehmer sequence* $R(L,M)$ *such that* $\gcd(L,M) = 1$. *Then* $R_{25}(L,M)| = p$ *only if* $(L,M) = (F_{k-2\varepsilon}, F_k)$ *for some* $k \geq 3$ *and* ε. *Moreover, the set of primes* p *for which* $|R_{25}(L,M)| = p$ *for some standard ordered pair* (L,M) *has natural density* 0 *in the set of primes.*

3. Preliminaries and Auxiliary Results

Definition 3.1. Let $\{W_n\}_{n=0}^{\infty}$ be a sequence of integers. Then p is a *primitive prime divisor* of W_n for $n \geq 1$ if $p \mid W_n$ and either $n = 1$ or $n \geq 2$ and $p \nmid W_1W_2 \cdots W_{n-1}$.

A key tool in finding composite indices n for which $|R_n(L,M)| = p$ or $|U_n(P,Q)| = p$ is the following theorem, which is proved in Theorems C, 1.3, and 1.4 by Bilu, Hanrot, Voutier in [1].

Theorem 3.2. *Let us consider the nondegenerate Lehmer and Lucas sequences* $R(L,M)$ *and* $U(P,Q)$ *for which* $\gcd(L,M) = \gcd(P,Q) = 1$. *Let* $P_n = U_n(2,-1)$ *and* $Q_n = \frac{1}{2}V_n(2,-1)$.

(i) *If* $n > 30$, *then both* R_n *and* U_n *have a primitive prime divisor.*
(ii) *If* $n \leq 30$, *then* R_n *has a primitive prime divisor unless*

$$n \in \{1, \ldots, 10, 12, \ldots, 15, 18, 24, 26, 30\}.$$

(iii) *If* $n \le 30$*, then* U_n *has a primitive prime divisor if it is not the case that* $n \in \{1, \dots, 8, 10, 12, 13, 18, 30\}$.

(iv) *If* $n \in \{7, 9, 13, 14, 15, 18, 24, 26, 30\}$*, then there are exactly* 22 *terms such that* $R_n(L, M)$ *has no primitive prime divisors. These terms are given in Table 1 below, which is extracted from Table 2 on page 78 of* [1].

(v) *If* $n \in \{5, 8\}$*, then there are infinitely many terms such that* $R_n(L, M)$ *has no primitive prime divisors. These terms are also given in Table 1 below, which is extracted from Table 4 on page 79 of* [1].

Table 1. Values for which $R_n(L, M)$ has no primitive prime divisor when n = 5, 7, 8, 9, 13, 14, 15, 18, 24, 26, or 30.

n	(L, M)
5	$(F_{k-2\varepsilon}, F_k)$ for $k \ge 3$
7	$(1,5)$, $(3,2)$, $(13,4)$, $(14,9)$
8	$(Q_{k-\varepsilon}, P_k)$ for $k \ge 2$
9	$(5,2)$, $(7,2)$, $(7,3)$
13	$(1,2)$
14	$(3,4)$, $(5,2)$, $(19,5)$, $(22,9)$
15	$(7,2)$, $(10,3)$
18	$(1,2)$, $(3,2)$, $(5,3)$
24	$(3,2)$, $(5,2)$
26	$(7,2)$
30	$(1,2)$, $(2,3)$

If R_n, (respectively U_n) has no primitive prime divisor, we say that R_n, (respectively U_n) is *defective*.

Remark 3.3. As contrasted to our definition of a primitive prime divisor, Bilu, Hanrot, and Voutier in [1] define p to be a primitive prime divisor of R_n, (respectively, U_n) if $p \mid R_n$, (respectively, $p \mid U_n$), but $p \nmid KLR_1R_2 \cdots R_{n-1}$ (respectively, $p \nmid DU_1U_2 \cdots U_{n-1}$). We will make use of Theorem 3.2 in the following manner. Suppose that $|R_n| = p$, where n is composite and $k > 1$ is a proper divisor of n. Then by Proposition 1.2 (i), $R_k \mid R_n$. This implies that either $|R_k| = 1$ and R_k is defective, or $|R_k| = p$ and R_n is defective. Similar considerations will be made in seeking composite n for which $|U_n| = p$.

The following results will be needed for the proofs of our main theorems.

Proposition 3.4. *Consider the Lehmer sequences* $R(L, M)$ *and* $S(L, M)$*. Then*

(i) $\gcd(R_m, R_n) = |R_d|$*, where* $d = \gcd(m, n)$,

(ii) $\gcd(R_n, S_n) \in \{1, 2\}$,

(iii) $R_{4n+1}(L, M) = -LMR_{2n}^2(L, M) + R_{2n+1}^2(L, M)$.

(iv) *The odd primitive prime divisors of* $R_n(L, M)$ *are of the form* $kn \pm 1$.

(v) *If* 2 *is a primitive prime divisor of* $R_n(L, M)$*, then* $n = 3$ *or* 4.

Proof. Parts (i) and (ii) are proved on page 421 of [5]. Part (iii) follows from (1.1). Parts (iv) and (v) are proved in [5], pp. 421 and 425. □

Proposition 3.5. *Consider the Lehmer sequences* $R(L, M)$ *and* $S(L, M)$*. Suppose that* $K(L, M) = L - 4M < 0$ *and* $n \geq 0$*. Then*

(i) $R_{2n+1}(L, M) = (-1)^n S_{2n+1}(|L - 4M|, M)$,
(ii) $R_{2n}(L, M) = (-1)^{n+1} R_{2n}(|L - 4M|, M)$,
(iii) $S_{2n}(L, M) = (-1)^n S_{2n}(|L - 4M|, M)$.

Proof. Parts (i)–(iii) follow from the formulas in (1.1). □

Remark 3.6. It can be easily seen that if $L > 0$ and $K(L, M) = L - 4M < 0$, then $K(|L - 4M|, M) < 0$ and $|K(|L - 4M|, M)| = L$.

Lemma 3.7. *Consider the Lehmer sequence* $R(L, M)$*. Then*

(i) $R_{2n}(L, M) \equiv L^{n-1} \pmod{M}$ *for* $n \geq 1$,
(ii) $R_{2n+1}(L, M) \equiv L^n \pmod{M}$ *for* $n \geq 0$.

Proof. Noting that $R_1 = R_2 = 1$, we find that parts (i) and (ii) follow by induction upon use of the recursion relation (1.3) defining $R(L, M)$. □

Proposition 3.8. *Consider the Fibonacci sequence* $\{F_n\}$ *and the Lucas sequence* $\{L_n\}$*. Then*

(i) $F_{n-1} + F_{n+1} = L_n$,
(ii) $F_n^2 + F_{n+1}^2 = F_{2n+1}$,
(iii) $L_n^2 + L_{n+1}^2 = 5F_{2n+1}$,
(iv) $F_m L_n + F_n L_m = 2F_{m+n}$,
(v) $F_{n-k}F_{n+k} - F_n^2 = -1^{n+k+1}F_k^2$,
(vi) $F_{n-2}F_{n+2} - F_n^2 = (-1)^{n+1}$.

Proof. Identities (i)–(iv) are proved in [10], pp. 176–177. Identity (v) is (I_{19}) on page 59 of [4] and (vi) follows from (v) upon letting $k = 2$. □

Lemma 3.9. *Consider the Lehmer sequence* $R(L, M)$*. Then*

$$R_5(L_{k+\varepsilon}, F_k) = -R_5(L_k, F_{k+\varepsilon}).$$

Proof. It follows from Example 1.1 and parts (ii)–(iv) of Proposition 3.8 that

$$R_5(L_{k+\varepsilon}, F_k) + R_5(L_k, F_{k+\varepsilon}) = (L_{k+\varepsilon}^2 - 3L_{k+\varepsilon}F_k + F_k^2) + (L_k^2 - 3L_kF_{k+\varepsilon} + F_{k+\varepsilon}^2)$$
$$= (L_{k+\varepsilon}^2 + L_k^2) + (F_{k+\varepsilon}^2 + F_k^2) - 3(L_{k+\varepsilon}F_k + L_kF_{k+\varepsilon}) = 5F_{2k+\varepsilon} + F_{2k+\varepsilon} - 6F_{2k+\varepsilon} = 0.$$

□

Lemma 3.10. *We have*

(i) $F_n - 4F_{n+2} = -L_{n+3}$,
(ii) $F_{n+2} - 4F_n = -L_{n-1}$.

Proof.

(i) By Proposition 3.8 (i), we see that

$$F_n - 4F_{n+2} = (F_n - F_{n+2}) - F_{n+2} - 2F_{n+2} = (-F_{n+1} - F_{n+2}) - F_{n+2} - F_{n+2}$$
$$= (-F_{n+3} - F_{n+2}) - F_{n+2} = -(F_{n+4} + F_{n+2}) = -L_{n+3}.$$

(ii) Moreover,

$$F_{n+2} - 4F_n = (F_{n+2} - F_n) - F_n - 2F_n = (F_{n+1} - F_n) - F_n - F_n$$
$$= (F_{n-1} - F_n) - F_n = -(F_{n-2} + F_n) = -L_{n-1}.$$

□

Lemma 3.11. *Let* $P_n = U_n(2,-1)$ *and* $Q_n = \frac{1}{2}V_n(2,-1)$. *Then*

(i) Q_n *is odd for* $n \geq 0$,
(ii) $Q_{n-\varepsilon} - 2P_n = -\varepsilon Q_n$,
(iii) $Q_{n-\varepsilon} - 4P_n = -Q_{n+\varepsilon}$,
(iv) $Q_{2n} = 2Q_n^2 - (-1)^n$.

Proof. Parts (i)–(iii) can be established by induction upon using the recursion relation defining both $\{P_n\}$ and $\{Q_n\}$. Part (iv) follows from Proposition 1.2 (vii). □

Lemma 3.12. *Consider the sequence* $W(P,Q) = \{W_n\}_{n=0}^{\infty}$ *satisfying the second-order recursion relation*

$$W_{n+2} = PW_{n+1} - QW_n,$$

where W_0, W_1, P, *and* Q *are rational integers,* $P > 0$, *and* $Q \neq 0$. *Suppose that* $D(P,Q) = P^2 - 4Q > 0$, $W_1 \geq PW_0/2$, $W_0 \geq 0$, *and* $W_1 \neq 0$. *Then the sequence* $W(P,Q)$ *is increasing for* $n \geq 2$. *Moreover, if* $P \geq 2$, *then* $W(P,Q)$ *is increasing for* $n \geq 1$, *while if* $P \geq 3$ *then* $W(P,Q)$ *is increasing for* $n \geq 0$.

Lemma 3.12 follows from the proof of Lemma 3 in [3].

Lemma 3.13. *Consider the Lehmer sequences* $R(L,M)$ *and* $S(L,M)$, *where* $LM \neq 0$ *and* $K(L,M) = L - 4M > 0$. *Let* $W_n = R_{2n}$, $\overline{W}_n = S_{2n}$, $X_n = R_{2n+1}$, *and* $\overline{X}_n = S_{2n+1}$ *for* $n \geq 0$. *Then* $\{W_n\}_{n=0}^{\infty}$,$\{\overline{W}_n\}_{n=0}^{\infty}$, $\{X_n\}_{n=0}^{\infty}$, *and* $\{\overline{X}_n\}_{n=0}^{\infty}$ *are increasing sequences.*

Proof. Note that $W_0 = 0$, $W_1 = 1$, $\overline{W}_0 = 2$, $\overline{W}_1 = L - 2M$, $X_0 = 1$, $X_1 = L - M$, and $\overline{X}_0 = 1$, $\overline{X}_1 = L - 3M$. By (1.1)

$$W_n = \frac{1}{\gamma^2 - \delta^2}\left(\gamma^2\right)^n - \frac{1}{\gamma^2 - \delta^2}\left(\delta^2\right)^n,$$

$$\overline{W}_n = \left(\gamma^2\right)^n + \left(\delta^2\right)^n,$$

$$X_n = \frac{\gamma}{\gamma - \delta}\left(\gamma^2\right)^n - \frac{\delta}{\gamma - \delta}\left(\delta^2\right)^n,$$

and

$$\overline{X}_n = \frac{\gamma}{\gamma + \delta}\left(\gamma^2\right)^n + \frac{\delta}{\gamma + \delta}\left(\delta^2\right)^n.$$

Thus, $\{W_n\}$, $\{\overline{W}_n\}$, $\{X_n\}$, and $\{\overline{X}_n\}$ all satisfy the second-order recursion relation

$$Y_{n+2} = (\gamma^2 + \delta^2)Y_{n+1} - \gamma^2\delta^2 Y_n,$$

where the parameters

$$\gamma^2 + \delta^2 = (\gamma + \delta)^2 - 2\gamma\delta = (\sqrt{L})^2 - 2M = L - 2M$$

and $\gamma^2\delta^2 = M^2$ are positive rational integers and the discriminant

$$D(L - 2M, M^2) = (L - 2M)^2 - 4M^2 = L(L - 4M) = L \cdot K(L,M) > 0.$$

Note that since $L - 4M > 0$, we have

$$W_1 = 1 > \frac{L - 2M}{2} W_0 = 0,$$

$$\overline{W}_1 = L - 2M = \frac{L - 2M}{2}\overline{W}_0,$$

$$X_1 = L - M > \frac{L-2M}{2} X_0 = \frac{L}{2} - M,$$
$$\overline{X}_1 = L - 3M > \frac{L-2M}{2} \overline{X}_0 = \frac{L}{2} - M.$$

Since $L - 2M \geq 3$, it follows from Lemma 3.12 that $\{W_n\}$, $\{\overline{W}_n\}$, $\{X_n\}$, and $\{\overline{X}_n\}$ are all increasing sequences. □

Lemma 3.14. *Let $R(L, M)$ and $U(P, Q)$ be nondegenerate Lehmer and Lucas sequences for which* $\gcd(L, M) = \gcd(P, Q) = 1$.

(i) *Suppose that $n \geq 4$, R_n has a primitive prime divisor p and there exists an integer m such that $2 < m < n$, $m \mid n$, and $|R_m| \geq 2$. Then $|R_n|$ is not prime and $R_n \neq 0$.*
(ii) *Suppose that $n \geq 4$, U_n has a primitive prime divisor p and there exists an integer m such that $2 \leq m < n$, $m \mid n$, and $|U_m| \geq 2$. Then $|U_n|$ is not prime and $U_n \neq 0$.*

Proof. (i) Since $R(L, M)$ is nondegenerate, $R_n \neq 0$. Note that $pR_m \mid R_n$. Thus, R_n is not prime.

The proof of part (ii) is completely similar. □

Theorem 3.15. *Consider the nondegenerate Lehmer and Lucas sequences $R(L, M)$, $S(L, M)$, $U(P, Q)$, and $V(P, Q)$, where* $\gcd(L, M) = \gcd(P, Q) = 1$. *Let $P_k = U_k(2, -1)$, $Q_k = \frac{1}{2}V_k(2, -1)$, and $F_k = U_k(1, -1)$. Then $|R_n|$, $|S_n|$, $|U_n|$, or $|V_n| = 1$ if and only if one of the following holds:*

(i) $n = 1$, $R_1 = U_1 = S_1 = 1$,
(ii) $n = 1$, $P = 1$, $V_1 = 1$,
(iii) $n = 2$, $R_2 = 1$,
(iv) $n = 2$, $M \geq 2$, $L = 2M + \varepsilon$, $|S_2| = 1$,
(v) $n = 2$, $P = 1$, $U_2 = 1$,
(vi) $n = 2$, P *is odd*, $P \geq 3$, $Q = \frac{P^2-\varepsilon}{2}$, $|V_2| = 1$,
(vii) $n = 3$, $M \geq 2$, $L = M + \varepsilon$, $|R_3| = 1$,
(viii) $n = 3$, $M \geq 2$, $L = 3M + \varepsilon$, $|S_3| = 1$,
(ix) $n = 3$, $(P, \varepsilon) \neq (1, 1)$, $Q = P^2 - \varepsilon$, $|U_3| = 1$,
(x) $n = 4$, $M \geq 2$, $L = 2M + \varepsilon$, $|R_4| = 1$,
(xi) $n = 4$, $(L, M) = (Q_{k-\varepsilon}, P_k)$, $k \geq 2$, $|S_4| = 1$,
(xii) $n = 4$, $(P, Q) = (1, 2)$, $V_4 = 1$,
(xiii) $n = 5$, $(L, M) = (F_{k-2\varepsilon}, F_k)$, $k \geq 3$, $|R_5| = 1$,
(xiv) $n = 5$, $(L, M) = (|F_{k-2\varepsilon} - 4F_k|, F_k)$, $k \geq 3$, $|S_5| = 1$,
(xv) $n = 5$, $(P, Q) = (1, 2)$, $(1, 3)$, $(12, 55)$ *or* $(12, 377)$, $|U_5| = 1$,
(xvi) $n = 7$, $(L, M) = (1, 5)$, $(3, 2)$, $(13, 4)$, *or* $(14, 9)$, $|R_7| = 1$,
(xvii) $n = 7$, $(L, M) = (19, 5)$, $(5, 2)$, $(3, 4)$, *or* $(22, 9)$, $|S_7| = 1$,
(xviii) $n = 7$, $(P, Q) = (1, 5)$, $U_7 = 1$,
(xix) $n = 13$, $(L, M) = (P, Q) = (1, 2)$, $R_{13}(1, 2) = U_{13}(1, 2) = -1$,
(xx) $n = 13$, $(L, M) = (7, 2)$, $S_{13} = -1$.

Proof. We assume throughout this proof that $R(L, M)$, $S(L, M)$, $U(P, Q)$, and $V(P, Q)$ are all nondegenerate and that $\gcd(L, M) = \gcd(P, Q) = 1$. We prove the theorem for the Lehmer sequences $R(L, M)$ and $S(L, M)$. The results for the Lucas sequences $U(P, Q)$ and $V(P, Q)$ are proved as a special case of Lemma 2.21 in [6] and also follow from the results for $R(L, M)$ and $S(L, M)$ upon the use of (1.8) and (1.9). We note that by Lemma 3.13, if $K(L, M) > 0$, then $|R_n(L, M)| \geq 2$ for $n \geq 3$ and $|S_n(L, M)| \geq 2$ for $n \geq 2$.

We further note that if $|R_n| = 1$, then $R_n(L,M)$ has no primitive prime divisor, while the identity $R_{2n} = R_n S_n$ implies that if $|S_n| = 1$ then $R_{2n}(L,M)$ has no primitive prime divisor. By Theorem 3.2, it thus follows that if $|R_n| = 1$ then $n \in T_1 = \{1,\ldots,10,12,\ldots,15,18,24,26,30\}$ while if $|S_n| = 1$, then $n \in T_2 = \{1,\ldots,7,9,12,13,15\}$. Moreover, by Theorem 3.2 (iv) there are exactly 22 triples (n,L,M) such that $R_n(L,M)$ is defective (see Table 1) when

$$n \in \{7,9,13,14,15,18,24,26,30\}.$$

Observing that $R_1 = R_2 = S_1 = 1$, $S_2 = R_4 = L-2M$, $R_3 = L-M$, and $S_3 = L-3M$, we find by use of Lemma 1.4 (i) that parts (i), (iii), (iv), (vii), (viii), and (x) give all the possibilities for which $|R_n| = 1$ for $n \le 4$ and $|S_n| = 1$ for $n \le 3$.

We now find all instances in which $|R_n(L,M)| = 1$ for $n \ge 5$, n odd, and $n \in T_1$. By our discussion above, we must then have that $K(L,M) < 0$. Since $|R_n(L,M)| = |S_n(|L-4M|,M)|$ if both n is odd and $K(L,M) < 0$ by Proposition 3.5 (i), our results concerning $R_n(L,M)$ will also allow us to determine all cases such that $|S_n(L,M)| = 1$ when $n \ge 5$ is an odd integer. If n is an odd prime, it follows from Proposition 3.4 (i) and the fact that $R_1 = 1$ that if R_n has no primitive prime divisor, then $R_n = \pm 1$.

Observing that if $n \ge 5$ is prime and $n \in T_1$, then $n = 5, 7$, or 13, we see by Table 1 that parts (xiii), (xiv), (xvi), (xvii), (xix), and (xx) present all the possibilities in which $n \ge 5$ is prime and either $|R_n(L,M)| = 1$ or $|S_n(L,M)| = 1$.

The remaining cases in which n is odd and $n \in T_1$ are $n = 9$ or 15. Examining the 5 cases which are left in Table 1 for which $n \in \{9,15\}$ and $R_n(L,M)$ is defective, we find that $|R_n(L,M)| > 1$ in these instances. We have now treated all the cases for which $n \ge 5$ is odd and $n \in T_1$ or T_2.

We now suppose that n is even and either $n \in T_1$ for $n \ge 6$ or $n \in T_2$ for $n \ge 4$. We first search for all standard ordered pairs (L,M) for which $S_4(L,M) = \pm 1$. This can occur only if $S_4(L,M)$ is odd and $R_8(L,M)$ has no primitive divisor. First suppose that

$$S_4(L,M) = L^2 - 4LM + 2M^2$$

is odd. This can happen if and only if L is odd.

Now suppose that $R_8(L,M)$ is defective and L is odd. We observe by Proposition 3.4 (ii) that $\gcd(R_4(L,M), S_4(L,M)) = 1$, since S_4 is odd. Moreover, if d is any proper divisor of 8, then $d \mid 4$, which implies that $R_d \mid R_4$ by Proposition 1.2 (i). Hence, by Proposition 3.4 (i), $\gcd(R_m(L,M), S_4(L,M)) = 1$ for $1 \le m < 8$, since $S_4 \mid R_8$. Thus, $R_8(L,M)$ is defective when L is odd if and only if $S_4(L,M) = \pm 1$. By use of Lemma 3.11 (i) and Table 1, we see that part (xi) gives all cases for which $|S_4(L,M)| = 1$.

We now show that $|R_n(L,M)| > 1$ and $|S_n(L,M)| > 1$ for all the other even values of n in T_1 and T_2, respectively. We first treat the companion Lehmer sequence $S(L,M)$. Suppose that

$$S_6(L,M) = L^3 - 6L^2M + 9LM^2 - 2M^3 = (L-2M)(L^2 - 4LM + M^2) = \pm 1.$$

Then $L - 2M = \varepsilon$ and

$$L^2 - 4LM + M^2 = \pm 1. \tag{3.1}$$

Substituting $L = 2M + \varepsilon$ into (3.1), we obtain that

$$-3M^2 + 1 = \pm 1,$$

which implies that $M = 0$, which is a contradiction, or $M^2 = 2/3$, which is impossible. Thus, $|S_6(L,M)| \ne 1$ for all standard ordered pairs (L,M).

The remaining even value of n in T_2 is $n = 12$. There are exactly two standard ordered pairs (L, M) in Table 1 for which $R_{24}(L, M)$ is defective. Checking both these ordered pairs, we see that $|S_{12}(L, M)| \neq 1$ in either case. We have now completely treated all the cases for which $n \in T_2$.

Now suppose that $|R_n(L, M)| = 1$, where $n \geq 6$ is even and $n \in T_1$. We first consider the case in which $|R_6(L, M)| = 1$. Then

$$R_6(L, M) = R_3(L, M)S_3(L, M) = (L - M)(L - 3M) = \pm 1.$$

Thus, $L - M = \pm 1$ and $L - 3M = \pm 1$. Since $L > 0$ and $M \neq 0$, we have that $M > 0$. Hence,

$$R_3(L, M) - S_3(L, M) = 2M \in \{-2, 0, 2\},$$

which implies that $M = 0$ or $(L, M) = (2, 1)$, both of which contradict the fact that $R(L, M)$ is nondegenerate. Since $R_6(L, M)|R_{6m}(L, M)$, we see that $|R_n(L, M)| = 1$ never occurs for $n = 6, 12, 18, 24$, or 30.

Next suppose that $|R_8(L, M)| = 1$. Then

$$R_8(L, M) = R_4(L, M)S_4(L, M) = (L - 2M)(L^2 - 4LM + 2M^2) = \pm 1.$$

Thus, $L - 2M = \varepsilon$ and

$$L^2 - 4LM + 2M^2 = \pm 1. \tag{3.2}$$

We again note that $M > 0$, since $L > 0$ and $M \neq 0$. Substituting $L = 2M + \varepsilon$ into (3.2), we get

$$-2M^2 + 1 = \pm 1.$$

Then $M = 0$, which is impossible, or $(L, M) = (1, 1)$ or $(3, 1)$, both of which contradict the fact that $R(L, M)$ is nondegenerate.

We now suppose that $|R_{10}(L, M)| = 1$. Then

$$R_{10}(L, M) = R_5(L, M)S_5(L, M) = (L^2 - 3LM + M^2)(L^2 - 5LM + 5M^2) = \pm 1.$$

Hence, $R_5(L, M) = \pm 1$, $S_5(L, M) = \pm 1$, and

$$R_5(L, M) - S_5(L, M) = 2LM - 4M^2 = 2M(L - 2M) \in \{-2, 0, 2\}.$$

Thus, $M \in \{-1, 0, 1\}$, since $\gcd(L, M) = 1$. Clearly, $M \neq 0$. Hence, $M = \pm 1$. If $M = 1$, then $L - 2M \in \{-1, 0, 1\}$, which implies that $(L, M) = (2, 1)$, $(3, 1)$, or $(1, 1)$, each of which contradicts the fact that $R(L, M)$ is nondegenerate. If $M = -1$, then $L < 0$, which contradicts the assumption that $L > 0$.

We finally suppose that $|R_n(L, M)| = 1$, where $n = 14$ or 26. By Table 1, there are five instances in which $R_n(L, M)$ is defective when $n = 14$ or 26. Examining each of these cases, we see that $|R_n(L, M)| > 1$, and the proof is complete. □

4. Proofs of the Main Theorems

In this section we prove the main results of this paper which have not already been proved in Section 2.

Proof of Theorem 2.4. (i) First suppose that the Lehmer sequence $R(L, M)$ has discriminant $K(L, M) > 0$. Suppose that $n > 4$ and n is composite. If $n \neq 2p$, then n has a factor a such that $2 < a < n$ and $a \equiv n \pmod 2$. Then by Proposition 1.2 (i) and Lemma 3.13, $R_a \mid R_n$ and $1 < R_a < R_n$. Hence, R_n is composite. If $n = 2p$, where $p \geq 3$, then by Proposition 1.2 (v) and Lemma 3.13, $R_{2p} = R_pS_p$, where $R_p > 1$ and $S_p > 1$, and R_n is again composite.

Now suppose that the Lucas sequence $U(P,Q)$ has discriminant $D(P,Q) > 0$. Assume that $n > 4$ and n is composite. Then n has a factor b such that $2 < b < n$. By Proposition 1.2 (i) and Lemma 3.12, $U_b \mid U_n$ and $1 < U_b < U_n$, and U_n is composite.

(ii) Note that $R_4 = L - 2M$. Thus, $|R_4| = p$ only if $L = 2M \pm p$. If $L = 2M - p$, then $M > 0$, since $L > 0$. However, then $K(L,M) = L - 4M < 0$, contradicting our hypothesis. Hence, $L = 2M + p$. If $p = 2$, then $M > 0$, since $R(L,M)$ is nondegenerate and $L > 0$. However, then $K(L,M) = L - 4M \leq 0$, which again is a contradiction. Therefore, p is odd. By the constraints, $L > 0$ and $L - 4M > 0$, we see that $-(p-1)/2 \leq M \leq (p-1)/2$.

(iii) Notice that $U_4 = P^3 - 2PQ = P(P^2 - 2Q)$. Thus, $|U_4| = p$ only if $P(P^2 - 2Q) = \pm p$. Since $P > 0$, we must have that $P = 1$ and $P^2 - 2Q = \pm p$ or $P = p$ and $P^2 - 2Q = \pm 1$. However, if $P^2 - 2Q = \pm 1$ or $-p$, then $D(P,Q) = P^2 - 4Q < 0$, which is a contradiction. Hence, $P = 1$ and $P^2 - 2Q = p$. Consequently, p is odd. Since $P^2 - 2Q = 1 - 2Q = p$, we see that $Q = (1-p)/2 < 0$. Since $Q < 0$, we observe that $D(P,Q) = P^2 - 4Q > 0$, as required. □

Proof of Theorem 2.5. We assume throughout this proof that $R(L,M)$ and $S(L,M)$ are both nondegenerate and that $\gcd(L,M) = 1$. We can also assume that $n \geq 12$, n is composite, and $|R_n(L,M)|$ is prime. We note that by Theorem 2.4 (i), we must have that $K(L,M) < 0$.

We first show that if n is composite, $n \geq 12$, and $n \notin \{14, 15, 21, 25, 26, 49, 65\}$, then $R_n(L,M)$ is never prime. Suppose that $n = 2k$, where $k \geq 6$ and $k \notin \{7, 13\}$. Then by Theorem 3.15, $|R_k(L,M)| \geq 2$ and $|S_k(L,M)| \geq 2$ for all standard ordered pairs (L,M). Thus, $|R_{2k}(L,M)| = |R_k(L,M)||S_k(L,M)|$ is not prime.

Now suppose that $|R_n|$ is prime, where n is a composite odd integer such that $n \geq 27$ and $n \notin \{49, 65\}$. Observe that $R_n(L,M)$ has a primitive prime divisor by Theorem 3.2. It thus follows from Lemma 3.14 (i) that $|R_m| = 1$ for each proper divisor $m > 1$ of n. By Theorem 3.15, $|R_m(L,M)| = 1$ for $m > 1$ an odd integer only if $m \in \{3, 5, 7, 13\}$. It follows that the sets of proper divisors of n which are greater than 1 are $\{3\}$, $\{5\}$, $\{7\}$, $\{13\}$, $\{3,5\}$, $\{3,7\}$, $\{3,13\}$, $\{5,7\}$, $\{5,13\}$, or $\{7,13\}$. We claim that it never happens that $|R_5(L,M)| = |R_7(L,M)| = 1$ or $|R_7(L,M)| = |R_{13}(L,M)| = 1$. If $|R_5(L,M)| = |R_7(L,M)| = 1$ then by Theorem 3.15 (xiii) and (xvi), $(L,M) = (F_{k-2\varepsilon}, F_k)$ for some $k \geq 3$ and also $(L,M) = (1,5)$, $(3,2)$, $(13,4)$, or $(14,9)$. This can never occur. If $|R_{13}(L,M)| = 1$, then by Theorem 3.15 (xix), $(L,M) = (1,2)$. However, $R_7(1,2) = 7$, and so we cannot have that $|R_7(L,M)| = |R_{13}(L,M)| = 1$.

Noting that $n \geq 27$ and $n \notin \{49, 65\}$, we see that $n = 39$ or $n = 169$. In both cases, we notice that $|R_{13}(L,M)| = 1$, which implies by our observation above that $(L,M) = (1,2)$. However, by the use of the computer algebra system GAP (Groups, Algorithms, and Programming), we observe that

$$|R_{39}(1,2)| = 24569 = 79 \cdot 311$$

and

$$|R_{169}(1,2)| = 3905547895493253204700049 = 264991 \cdot 14738417136782959439.$$

We now find all ordered pairs (L,M) such that $|R_n(L,M)$ is prime for $n = 14, 15, 21, 26, 49$, or 65. We first treat the even cases, $n = 14$ and $n = 26$. Recall that by Proposition 3.5 (ii), $|R_{2k}(L,M)| = |R_{2k}(|L-4M|, M)|$ when $K(L,M) < 0$. By our argument above, $|R_{14}(L,M)|$ is prime only if $|R_7(L,M)| = 1$ or $|S_7(L,M)| = 1$. By Theorem 3.15 (xvi) and (xvii), $|R_7(L,M)| = 1$ if and only if $(L,M) = (1,5)$, $(3,2)$, $(13,4)$, or $(14,9)$, while $|S_7(L,M)| = 1$ if and only if $(L, M) = (19, 5)$, $(5, 2)$, $(3, 4)$, or $(22, 9)$. We observe by inspection that

$$|R_{14}(1, 5)| = |R_{14}(19, 5)| = 559 = 13 \cdot 43,$$
$$|R_{14}(3, 2)| = |R_{14}(5, 2)| = 13,$$
$$|R_{14}(13, 4)| = |R_{14}(3, 4)| = 71,$$

and

$$|R_{14}(14, 9)| = |R_{14}(22, 9)| = 1169 = 7 \cdot 167.$$

Now, we will investigate the case in which $|R_{26}(L, M)|$ is prime. Then $|R_{13}(L, M)| = 1$ or $|S_{13}(L, M)| = 1$. By Theorem 3.15 (xix) and (xx), $|R_{13}(L, M)| = 1$ if and only if $(L, M) = (1, 2)$, whereas $|S_{13}(L, M)| = 1$ if and only if $(L, M) = (7, 2)$. We observe by inspection that $|R_{26}(1, 2)| = |R_{26}(7, 2)| = 181$, which is prime.

We now suppose that $|R_{15}(L, M)|$ is prime. By Lemma 3.14 (i), we must have that $R_{15}(L, M)$ has a primitive prime divisor and $|R_3(L, M)| = |R_5(L, M)| = 1$ or it is the case that $R_{15}(L, M)$ has no primitive prime divisor. Suppose that $R_{15}(L, M)$ has no primitive prime divisor. Then by Table 1, $(L, M) = (7, 2)$ or $(10, 3)$. We note that $|R_{15}(7, 2)| = 275 = 5^2 \cdot 11$, while $R_{15}(10, 3) = 133 = 7 \cdot 19$. Now suppose that $R_{15}(L, M)$ has a primitive prime divisor. We note by Theorem 3.15 (vii) and (xiii) that $|R_3(L, M)| = |R_5(L, M)| = 1$ if and only if $|L - M| = 1$ and $(L, M) = (F_{k-2\varepsilon}, F_k)$ for some $k \geq 3$. This occurs if and only if $(L, M) = (1, 2)$. We now observe that $R_{15}(1, 2)| = 89$, which is prime.

Next suppose that $|R_{21}(L, M)|$ is prime. By Theorem 3.2 (ii), $R_{21}(L, M)$ has a primitive prime divisor. Thus, we must have that $|R_3(L, M)| = |R_7(L, M)| = 1$. Then by Theorem 3.15 (vii) and (xvi), we see that $|L - M| = 1$ and $(L, M) = (1, 5)$, $(3, 2)$, $(13, 4)$, or $(14, 9)$. Hence, we need only consider the sequence $R(3, 2)$. We observe that $|R_{21}(3, 2)| = 379$, which is prime.

Now we suppose that $|R_{49}(L, M)|$ is prime. By Theorem 3.2, $R_{49}(L, M)$ has a primitive prime divisor. Thus, $|R_7(L, M)| = 1$ by Lemma 3.14 (i). According to Theorem 3.15 (xvi), this occurs only if $(L, M) = (1, 5)$, $(3, 2)$, $(13, 4)$, or $(14, 9)$. By use of GAP and *Mathematica*, we find that

$$|R_{49}(1, 5)| = 3336236769680641 = 491 \cdot 6794779571651,$$
$$|R_{49}(3, 2)| = 13555459 = 97 \cdot 139747,$$
$$|R_{49}(13, 4)| = 30775052320741,$$

which is prime, and

$$|R_{49}(14, 9)| = 765925877884715074799 = 2351 \cdot 325787272600899649.$$

Finally, we treat the case in which $|R_{65}(L, M)|$ is prime. By Theorem 3.2, $R_{65}(L, M)$ has a primitive prime divisor. Thus, $|R_5(L, M)| = |R_{13}(L, M)| = 1$. By Theorem 3.15 (xix), we find that $R_{13}(L, M) = 1$ if and only if $(L, M) = (1, 2)$. By inspection we see that $|R_5(1, 2)| = 1$ also. Using GAP, we find that $|R_{65}(1, 2)| = 335257649$, which is prime. □

Proof of Theorem 2.13. Suppose that

$$|R_8(L, M)| = |R_4(L, M)||S_4(L, M)| = |L - 2M||L^2 - 4LM + 2M^2| = p. \qquad (4.1)$$

Then either $R_4 = L - 2M = \varepsilon$ or $S_4 = L^2 - 4LM + 2M^2 = \pm 1$.

Suppose that $L = 2M + \varepsilon$. Then by (4.1),

$$|R_8(L, M)| = |\varepsilon||(2M + \varepsilon)^2 - 4(2M + \varepsilon)M + 2M^2| = | - 2M^2 + 1| = 2M^2 - 1 = p.$$

Since $L > 0$ and $R(L, M)$ is nondegenerate, we have $M \geq 2$. Then $|R_8(L, M)| = p$ if and only if $2M^2 - 1 = p$.

Now suppose that $L^2 - 4LM + 2M^2 = \pm 1$. By Theorem 3.15 (xi) this occurs if and only if $(L, M) = (Q_{k-\varepsilon}, P_k)$, where $k \geq 2$. Then by Proposition 3.5 (ii) and Lemma 3.11 (ii) and (iii),

$$\begin{aligned}|R_8(L, M)| &= |R_8(Q_{k-\varepsilon}, P_k)| = |R_4(Q_{k-\varepsilon}, P_k)| = |Q_{k-\varepsilon} - 2P_k| \\ &= Q_k = |R_8(|Q_{k-\varepsilon} - 4P_k|, P_k)| = |R_8(Q_{k+\varepsilon}, P_k)|.\end{aligned}$$

Parts (i) and (ii) are now established.

We now show that the set of primes p such that $|R_8(L, M)| = p$ for some standard ordered pair (L, M) has natural density 0 in the set of primes. Let $\pi(N)$ denote the number of primes less than or equal to N. Then by the Prime Number Theorem, $\pi(N) \sim N/\ln N$. Let G_n denote the nth prime of the form $2M^2 - 1$, where $M \geq 2$. Then $G_n \geq n^2$ for $n \geq 1$. Let H_n denote the nth prime of the form $Q_k = \frac{1}{2}V_k(2, -1)$, where $k \geq 2$. Then

$$Q_k = \frac{1}{2}(\alpha^k + \beta^k) = \frac{1}{2}((1 + \sqrt{2})^k + (1 - \sqrt{2})^k).$$

We observe that $1 + \sqrt{2} > 2.4$ and $-0.5 < 1 - \sqrt{2} < 0$. Thus, $|(1 - \sqrt{2})^n| < 1$ for $n \geq 1$. Hence, $H_n \geq \frac{1}{4}(1 + \sqrt{2})^n$ for $n \geq 1$. Let $A(N)$ denote the number of primes of the form $2M^2 - 1$ which are less than or equal to N and let $B(N)$ denote the number of primes of the form Q_k which are less than or equal to N. Hence, by the above inequalities,

$$A(N) \leq \sqrt{N}$$

and

$$B(N) \leq \log_{1+\sqrt{2}}(4N) = \frac{\ln 4 + \ln N}{\ln(1 + \sqrt{2})}.$$

Hence, the natural density in the set of primes of those primes of the form $2M^2 - 1$ or Q_k is less than or equal to

$$\lim_{N\to\infty} \frac{\sqrt{N} + \ln 4 + \ln N}{N/\ln N} = 0.$$

Thus, the desired natural density is indeed equal to 0. □

Proof of Theorem 2.14. Suppose that $|R_9(L, M)| = p$. Either $|R_9(L, M)|$ has a primitive prime divisor or $R_9(L, M)$ is defective.

Suppose first that $R_9(L, M)$ is defective. By Table 1 we must have that $(L, M) = (5, 2)$, $(7, 2)$, or $(7, 3)$. By inspection, we see that $R_9(5, 2) = -9$, $R_9(7, 2) = -5$,, and $R_9(7, 3) = 4$. Thus, $|R_9(L, M)|$ is prime and defective if and only if (i) holds.

Now suppose that $R_9(L, M)$ is nondefective. Then by Lemma 3.14 (i), $R_3(L, M) = L - M = \varepsilon$. If $L = M - 1$, then by Proposition 3.4 (iii),

$$\begin{aligned}|R_9(L, M)| &= |R_9(M - 1, M)| = | - M(M - 1)R_4^2(M - 1, M) + R_5^2(M - 1, M)| \\ &= | - M(M - 1)(-M - 1)^2 + ((M - 1)^2 - 3M(M - 1) + M^2)^2| \\ &= | - 3M(M^2 - 1) + 1| = 3M(M^2 - 1) - 1.\end{aligned}$$

If $L = M + 1$, then again by Proposition 3.4 (iii),

$$\begin{aligned}|R_9(L, M)| &= |R_9(M + 1, M)| = | - M(M + 1)R_4^2(M + 1, M) + R_5^2(M + 1, M)| \\ &= | - M(M + 1)(-M + 1)^2 + ((M + 1)^2 - 3M(M + 1) + M^2)^2| \\ &= 3M(M^2 - 1) + 1 = |R_9(M - 1, M)| + 2.\end{aligned}$$

We note that $M \geq 2$, since $L > 0$ and $R(L, M)$ is nondegenerate. Parts (ii) and (iii) are now established. It now immediately follows from (1.8) that $|U_9(P, Q)| = p$ if and only if $(P, Q) = (M, M^2 + \varepsilon)$ for some $M \geq 1$ such that $(P, Q) \neq (1, 0)$, and (2.5) holds.

We now show that the set of primes p for which $|R_9(L, M)| = p$ or $|U_9(P, Q)| = p$ for some standard ordered pair (L, M) or (P, Q) indeed has natural density 0 in the set of primes. Since $|U_9(P, Q)| = |R_9(P^2, Q)|$ by (1.8), it suffices to establish the natural density for the Lehmer numbers $|R_9(L, M)|$ which are prime. By the earlier part of this proof, $|R_9(L, M)| = p$ only if $p = 5$ or p is of the form $3M(M^2 - 1) \pm 1$.

Let G_n denote the nth prime of the form $3M(M^2 - 1) - 1$ and H_n denote the nth prime of the form $3M(M^2 - 1) + 1$ for $M \geq 2$. Then $G_n \geq n^3$ and $H_n \geq n^3$ for all $n \geq 1$. Our result on the natural density now follows from a similar argument to that given in the proof of Theorem 2.13. □

Proof of Theorem 2.15. Suppose that $|R_{10}(L, M)| = p$. Since

$$|R_{10}(L, M)| = |R_5(L, M)||S_5(L, M)| = |L^2 - 3LM + M^2||L^2 - 5LM + 5M^2| = p,$$

we have $|R_5(L, M)| = |L^2 - 3LM + M^2| = 1$ and $|S_5(L, M)| = |L^2 - 5LM + 5M^2| = p$ or $|R_5(L, M)| = p$ and $|S_5(L, M)| = 1$. By Theorem 3.15 (xiii), $|R_5(L, M)| = 1$ for some standard ordered pair (L, M) if and only if

$$(L, M) = (F_{k-2\varepsilon}, F_k) \tag{4.2}$$

for some $k \geq 3$. We also see by Theorem 3.15 (xiv) and Lemma 3.10 that $|S_5(L, M)| = 1$ for some standard ordered pair (L, M) if and only if

$$(L, M) = (|F_{k-2\varepsilon} - 4F_k|, F_k) = (L_{k+\varepsilon}, F_k) \tag{4.3}$$

for some $k \geq 3$. However, by Proposition 3.5 (i), Remark 3.6, and Lemma 3.10,

$$|S_5(L_{k+\varepsilon}, F_k)| = |R_5(|L_{k+\varepsilon} - 4F_k|, F_k) = |R_5(F_{k-2\varepsilon}, F_k)|. \tag{4.4}$$

Thus, $|R_{10}(L, M)| = p$ for some standard ordered pair (L, M) if and only if there exists $k \geq 3$ such that

$$|S_5(F_{k-2\varepsilon}, F_k)| = |F_{k-2\varepsilon}^2 - 5F_{k-2\varepsilon}F_k + 5F_k^2| = p. \tag{4.5}$$

Now suppose that (4.5) holds for some $k \geq 3$. Then by (4.2), $|R_5(F_{k-2\varepsilon}, F_k)| = 1$ and it follows by Proposition 1.2 (v), (4.3), and Lemmas 3.9 and 3.10 that

$$\begin{aligned} p &= |S_5(F_{k-2\varepsilon}, F_k)| = |R_{10}(F_{k-2\varepsilon}, F_k)| = |R_5(L_{k+\varepsilon}, F_k)| = |R_{10}(L_{k+\varepsilon}, F_k)| \\ &= |R_5(L_k, F_{k+\varepsilon})| = |R_{10}(L_k, F_{k+\varepsilon})| = |R_{10}(|L_k - 4F_{k+\varepsilon}|, F_{k+\varepsilon})|. \end{aligned} \tag{4.6}$$

Then (2.7) will be established if we can show that

$$|L_k - 4F_{k+\varepsilon}| = F_{k+3\varepsilon}. \tag{4.7}$$

In equation (4.6), let $k = m - \varepsilon$ and $\tau = -\varepsilon$. Then by Lemma 3.10, we have

$$L_k - 4F_{k+\varepsilon} = L_{m-\varepsilon} - 4F_m = L_{m+\tau} - 4F_m = -F_{m-2\tau} = -F_{k+3\varepsilon},$$

and (4.6) holds. □

Proof of Corollary 2.16. We first establish that (2.8) holds. When $k = 2$, we note that while $R(F_0, F_2) = R(0, 1)$ is degenerate and $|R_{10}(0, 1)| = 5$, we also find that $R(5, 2)$ is nondegenerate and $|R_{10}(5, 2)| = 5$.

We now let $k \geq 3$. Let $m = k + 1$. Then $m \geq 4$. By Theorem 2.15, $|R_{10}(L, M)| = p$ if and only if there exist Fibonacci numbers $F_{m-2\varepsilon}$ and F_m such that

$$|S_5(F_{m-2\varepsilon}, F_m)| = p.$$

Moreover, by (4.6) and (4.7) in the proof of Theorem 2.15,

$$|S_5(F_{m+2}, F_m)| = |R_5(L_m, F_{m-1})|$$

and

$$|L_m - 4F_{m-1}| = F_{m-3}.$$

It follows from Proposition 3.5 (i) that

$$|R_5(L_m, F_{m-1})| = |S_5(F_{m-3}, F_{m-1})|.$$

Upon substituting m in terms of k and noting that $F_k > F_{k-2}$, we obtain

$$S_5(F_{k-2}, F_k) = F_{k-2}^2 - 5F_{k-2}F_k + 5F_k^2 = p$$

for $k \geq 2$ whenever $|S_5(F_{k+3}, F_{k+1})| = p$, and (2.8) now follows.

We now show that the set of primes p for which

$$|R_{10}(L, M)| = p \tag{4.8}$$

for some standard ordered pair (L, M) has natural density 0 in the set of primes. By our discussion above, (4.8) holds if and only if

$$\begin{aligned} S_5(F_{k-2}, F_k) &= F_{k-2}^2 - 5F_{k-2}F_k + 5F_k^2 \\ &= F_{k-2}^2 + 5F_k(F_k - F_{k-2}) = F_{k-2}^2 + 5F_{k-1}F_k = p \end{aligned} \tag{4.9}$$

for some $k \geq 2$.

Let G_n denote the nth prime of the form $S_5(F_{k-2}, F_k)$ for some $k \geq 2$. Then by (4.9) and the Binet formula given in (1.5),

$$G_n \geq 5F_n = \frac{5}{\sqrt{5}}\Big(\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big) > \frac{\sqrt{5}}{2}\Big(\frac{1+\sqrt{5}}{2}\Big)^n \tag{4.10}$$

for $n \geq 1$, since $1.6 < (1+\sqrt{5})/2 < 1.7$, $-0.7 < (1-\sqrt{5})/2 < 0$, and

$$\Big|\Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big| < 1.$$

The result on the natural density now follows from a similar argument to that given in the proof of Theorem 2.13. □

Proof of Theorem 2.17. By Theorem 3.2, $R_{25}(L, M)$ has a primitive prime divisor. It thus follows from Lemma 3.14 that $|R_5(L, M)| = 1$. However, according to Theorem 3.15 (xiii), $|R_5(L, M)| = 1$ for some standard ordered pair (L, M) if and only if $(L, M) = (F_{k-2\varepsilon}, F_k)$ for some $k \geq 3$.

We now demonstrate that the set of primes p for which

$$|R_{25}(L, M)| = p \tag{4.11}$$

for some standard ordered pair (L, M) has natural density 0 in the set of primes. By our above discussion, (4.11) holds only if $(L, M) = (F_{k-2\varepsilon}, F_k)$ for some $k \geq 3$. By Lemma 3.7 (ii) and Proposition 3.8 (vi),

$$R_{25}(F_{k-2\varepsilon}, F_k) \equiv F_{k-2\varepsilon}^{12} = (F_{k-2\varepsilon}^2)^6 \equiv (-1)^{6k} \equiv 1 \pmod{F_k}. \tag{4.12}$$

Let G_n denote the nth prime of the form $|R_{25}(F_{k-2\varepsilon}, F_k)|$ for some $k \geq 3$. By (4.12), $G_{2n-1} \geq F_n - 1$ and $G_{2n} \geq F_n + 1$. Since p is a primitive prime divisor of $R_{25}(L, M)$ if

$|R_{25}(L, M)| = p$, it follows from Proposition 3.4 (iv) and (v) that is p is odd and $p \equiv \pm 1 \pmod{50}$. We now see from (4.10) that

$$G_{2n} > G_{2n-1} \geq F_n - 1 > \frac{1}{4\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n$$

for $n \geq 3$. The result on the natural density now follows from a similar argument to that given in the proof of Theorem 2.13. □

5. Examples and Conjectures

Following Remark 2.12, we conjectured that for $k \in \{8, 9, 10, 25\}$, there exist infinitely many standard ordered pairs (L, M) for which $|R_k(L, M)|$ is prime. We provide justification for these conjectures by means of Schinzel's Hypothesis H (see [9]) and computer calculations using GAP and *Mathematica*.

Conjecture 5.1. (Schinzel's Hypothesis H.)

Let $f_1, f_2, \ldots, f_k$ be irreducible polynomials with integer coefficients such that the leading coefficient of each f_i is positive and such that for each prime p, there is some integer n with none of $f_1(n), f_2(n), \ldots, f_k(n)$ divisible by p. Then there are infinitely many positive integers n such that each $f_i(n)$ is prime.

Example 5.2. ($|R_8(L, M)| = p$.)

It follows from Theorem 2.13 that there exist infinitely many standard ordered pairs (L, M) such that $|R_8(L, M)|$ is prime if and only if either $2M^2 - 1$ is prime for infinitely many $M \geq 2$ or Q_k is prime for infinitely many $k \geq 2$. Schinzel's Hypothesis H implies that $2M^2 - 1$ is indeed prime for infinitely many values of M. It is also widely believed that Q_k is prime for infinitely many values of k (see [8], pp. 362–364).

By Theorem 2.13, we see that if $p = 2M^2 - 1$ or Q_k for some $M \geq 2$ or $k \geq 2$, then there exist two standard ordered pairs (L, M) such that $|R_8(L, M)| = p$. Additionally, if $Q_k = 2M^2 - 1$ for some $k \geq 2$ and $M \geq 2$, then there are exactly four standard ordered pairs (L, M) such that $|R_8(L, M)| = p$. For example, $Q_4 = 17 = 2 \cdot 3^2 - 1$ and

$$|R_8(5, 3)| = |R_8(7, 3)| = |R_8(7, 12)| = |R_8(41, 12)| = 17.$$

By Lemma 3.11 (iv), $Q_{4k} = 2Q_{2k}^2 - 1$.

It follows from Proposition 1.2 (ii) and Lemma 3.12 that Q_k can be prime only if k is a prime or a power of 2. By examination, we see that $Q_4 = 17$, $Q_8 = 577$, and $Q_{16} = 665867$ are all primes. Additionally, $Q_3 = 7 = 2 \cdot 2^2 - 1$ is also a prime. We conjecture that these four values are the only instances in which Q_k is a prime of the form $2M^2 - 1$. For k odd, Q_k is of the form $2M^2 - 1$ only for $k = 1, 3$. This follows from the theorem of Fermat, proved for example by T. Pepin (see [2], p. 487) that the system of Diophantine Equations $x = 2y^2 - 1$, $x^2 = 2z^2 - 1$ implies $x = 1$ or 7. Now, for k odd, $Q_k^2 = 2P_k^2 - 1$.

We tested the positive integers M up to 5600 and found that for $1326 = 23.68\%$ of these values, $2M^2 - 1$ is prime. It is known (see the website [13]) that Q_k is prime for 21 values, the largest of which is $k = 9679$ for which Q_k has 3705 digits.

Example 5.3. ($|R_9(L, M)| = p$ and $|U_9(P, Q)| = p$.)

By Theorem 2.14, $|R_9(L, M)| = p$ if and only if $p = 5$ or p is of the form

$$3M(M^2 - 1) + \varepsilon \tag{5.1}$$

for $M \geq 2$. If (5.1) holds, then by Theorem 2.14 (ii) and (iii), $|R_9(M+\varepsilon, M)| = p$. By Hypothesis H, there exist infinitely many pairs of twin primes $(p, p+2)$ such that $|R_9(M-1, M)| = p$ and $|R_9(M+1, M)| = p+2$ for $M \geq 2$. A fortiori, Hypothesis H implies that there are infinitely many primes p such that $|R_9(L, M)| = p$ for some standard ordered pair (L, M). Moreover, by Hypothesis H and (1.8), there are infinitely many values of M such that $|U_9(M, M^2+\varepsilon)| = |R_9(M^2, M^2+\varepsilon)|$ is prime.

We tested the terms $|R_9(M+\varepsilon, M)|$ for primality for $2 \leq M \leq 149380$. We determined that $|R_9(M+\varepsilon, M)|$ is prime for $39928 = 13.36\%$ of these 298758 ordered pairs $(M+\varepsilon, M)$. The largest prime value found for $|R_9(L, M)|$ was $|R_9(149373, 149372)| = 9998361674932429$. Moreover, for $2493 = 1.67\%$ of 149379 values of M for which $2 \leq M \leq 149380$, $|R_9(M-1, M)|$ and $|R_9(M+1, M)|$ form a pair of twin primes. The largest pair of twin primes found were

$$|R_9(149271, 149272)| = 9978294320467127$$

and

$$|R_9(149273, 149272)| = 9978294320467129.$$

By Theorem 2.14, $|U_9(P, Q)| = p$ if and only if $(P, Q) = (M, M^2+\varepsilon)$ for some M such that $M \geq 1$, $(P, Q) \neq (1, 0)$, and $|R_9(M^2, M^2+\varepsilon)| = p$. We found that for 121 ordered pairs $(M^2, M^2+\varepsilon)$ such that $M \leq 149380$ and $|R_9(M^2, M^2+\varepsilon)|$ is prime. The largest prime value found for $|U_9(P, Q)|$ was

$$|U_9(380, 14401)| = |R_9(14400, 14401)| = 9032996815106399.$$

Example 5.4. ($|R_{10}(L, M)| = p$.)

By Corollary 2.16, $|R_{10}(L, M)| = p$ for some standard ordered pair (L, M) if and only if

$$S_5(F_{k-2}, F_k) = F_{k-2}^2 - 5F_{k-2}F_k + 5F_k^2 = p$$

for some $k \geq 2$. We tested the expression $F_{k-2}^2 - 5F_{k-2}F_k + 5F_k^2$ for primality for $2 \leq k \leq 1000$. Twelve primes and eighteen probable primes were found. The largest prime found was

$$|R_{10}(F_{28}, F_{30})| = |S_5(F_{28}, F_{30})| = |R_{10}(317811, 832040)| = 2240299317521.$$

These computer results lend some credence to our conjecture that $|R_{10}(L, M)|$ is prime for infinitely many ordered pairs (L, M).

By Theorem 2.15, if $|R_{10}(L, M)| = p$ for some standard ordered pair (L, M), then there exist four distinct ordered pairs (L, M) such that $|R_{10}(L, M)| = p$. We verify this when $p = 79$. Then by inspection we see that

$$\begin{aligned}|R_{10}(F_3, F_5)| &= |R_{10}(2, 5)| = |R_{10}(L_6, F_5)| = |R_{10}(18, 5)| = |R_{10}(F_8, F_6)| \\ &= |R_{10}(21, 8)| = |R_{10}(L_5, F_6)| = |R_{10}(11, 8)| = 79.\end{aligned}$$

Example 5.5. ($|R_{25}(L, M)| = p$.)

By Theorem 2.17, $|R_{25}(L, M)| = p$ for some standard ordered pair (L, M) only if $(L, M) = (F_{k-2\varepsilon}, F_k)$ for some $k \geq 3$. We tested the terms $|R_{25}(F_{k-2\varepsilon}, F_k)|$ for primality for $3 \leq k \leq 1000$. We found 5 primes and 13 probable primes. The five primes found are $|R_{25}(1, 2)| = 4049$, $|R_{25}(5, 2)| = 4649$, $|R_{25}(1, 3)| = 282001$, $|R_{25}(21, 8)| = 5366907001$, and

$$|R_{25}(8, 21)| = 83397852938401.$$

One sees that the size of the primes p for which $|R_{25}(L, M)| = p$ appears to grow very rapidly. These computer results provide some plausibility for our conjecture that $|R_{25}(L, M)|$ is prime for infinitely many standard ordered pairs (L, M).

6. Acknowledgements

The authors would like to thank Walter Carlip (State Univ. of New York at Binghamton) for extensive calculations using GAP and *Mathematica*.

References

[1] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., **539** (2001), 75–122.
[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea Publ. Company, New York, 1971.
[3] P. Hilton, J. Pedersen, and L. Somer, *On Lucasian numbers*, The Fibonacci Quarterly, **35.1** (1997), 43–47.
[4] V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers*, Houghton Mifflin Company, Boston, 1969.
[5] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., **31** (1930), 419–448.
[6] F. Luca and L. Somer, *Lucas sequences for which* $4 \mid \phi(|u_n|)$ *for almost all* n, The Fibonacci Quarterly, **44.3** (2006), 249–263.
[7] B. M. Phong, *On super Lucas and super Lehmer pseudoprimes*, Studia Sci. Math. Hungar., **23** (1988), 435–442.
[8] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.
[9] A. Schinzel and W. Sierpiński, *Sur certain hypothèses concernant les nombres premiers*, Acta Arith., **4** (1958), 185–208; Erratum, ibid, **5** (1958), 259.
[10] S. Vajda, *Fibonacci & Lucas Numbers and the Golden Section*, Ellis Horwood Ltd., New York, 1989.
[11] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.
[12] E. W. Weisstein, *Fibonacci prime*, From MathWorld - A Wolfram web resource, `http://mathworld.wolfram.com/FibonacciPrime.html`.
[13] E. W. Weisstein, *Pell number*, From MathWorld - A Wolfram web resource, `http://mathworld.wolfram.com/PellNumber.html`.

MSC2010: 11B39, 11A41, 11A51

Department of Mathematics, Catholic University of America, Washington, D.C. 20064
E-mail address: somer@cua.edu

Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz